



## What is Application Whitelisting?

Application Whitelisting is a proactive security technique where only a limited set of approved programs are allowed to run, while all other programs (including most malware) are blocked from running by default. In contrast, the standard policy enforced by most operating systems allows all users to download and run any program they choose. Application Whitelisting enables only the administrators, not the users, to decide which programs are allowed to run.

Application Whitelisting is not a replacement for traditional security software, such as antivirus and host firewalls. It should be used as one layer in a defense-in-depth strategy. For an application whitelisting solution to be effective:

- All executable code must be blocked by default so only approved programs can run.
- Users must not be allowed to modify the files that are allowed to run.

## Why use Application Whitelisting?

The amount of malware on the Internet increases in volume and variety every day. Malware developers and antivirus vendors are in a never-ending arms race. Malware authors continuously modify their creations so they are not detected, and antivirus vendors update their software daily to detect new malware variants. Defending against these threats by blocking every known malware sample, a technique known as *blacklisting*, is a reactive technique that does not scale well to the increasing volume and variety of malware. It also does not protect against unknown malware. Many attacks use previously unknown vulnerabilities, also known as zero-day vulnerabilities, which cannot be prevented with blacklisting techniques.

Corporate and government networks are prime targets for attackers. They contain valuable proprietary or sensitive information and have a large, diverse attack surface for an adversary to exploit. Attacks have shifted from operating system attacks to application-based attacks. This change has left each individual user, and the applications they use, as the main attack vectors into the network.

Unauthorized applications have the potential to cause great harm to a computer and to the network to which it is connected. All applications have inherent security risks that must be accepted by the organization. Use of unauthorized applications can introduce unknown and unacceptable additional security risks. Application Whitelisting prevents the use of unauthorized applications, thereby limiting the attack surface to only security risks that the organization has chosen to accept.

## Advantages

- Blocks most current malware
- Prevents use of unauthorized applications
- Does not require daily definition updates
- Requires administrator installation and approval of new applications

## Disadvantages

- Requires performance overhead to enforce the whitelist (varies greatly depending on implementation)
- Requires regular maintenance of the whitelist to add new applications and remove ones that are no longer approved
- Causes some users to be annoyed because they cannot download and run applications at will



The Information  
Assurance Mission  
at NSA

## How to Enforce Application Whitelisting

There are several companies that have enterprise Application Whitelisting solutions. Most of the solutions make management of the whitelist easy for administrators, enable updating of applications, and monitor and report attempted violations of the policy. Many of these solutions are expensive, unlike the built-in (no additional cost) Software Restriction Policies on Windows computers.

## What is Software Restriction Policies?

Software Restriction Policies (SRP) is a feature of Windows XP and later operating systems. It can be configured to enforce an Application Whitelisting policy, enabling administrators to control which applications are allowed to run. It can be applied as either local policy or as domain policy to a network of Windows computers using Group Policy on Windows Server 2003 and later domains.

For the best balance of performance, security, and manageability, the NSA SNAC recommends employing path-based SRP rules to both executables and libraries. These rules have a minimal impact on system performance and allow most program updates and patches to be

applied without requiring any rule changes, while preventing the execution of new unauthorized programs and most current malware.

## Where to Find More Information

The SNAC's [Application Whitelisting using Software Restriction Policies](#) guidance document can be downloaded from:

[http://www.nsa.gov/ia/guidance/security\\_configuration\\_guides/operating\\_systems.shtml#microsoft](http://www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml#microsoft)

The document contains detailed instructions for developing an appropriate whitelist for a Windows network, configuring Software Restriction Policies, applying the rules across a Windows domain, maintaining the whitelist over time, and monitoring the enforcement of the policy.

# Application Whitelisting



Systems and Network Analysis Center (SNAC)  
National Security Agency  
9800 Savage Road  
Ft. Meade, MD 20755  
<http://www.nsa.gov/snac>